A Star-based Independent Biclique Attack on Full Rounds SQUARE

Zheng Yuan[1,2],✉ Zhen Peng[1,2],✉Ming Mao[1,2]

1. Beijing Electronic Science &Technology Institute, Beijing 100070,China
2. Xidian University, Xi'an , China

yuanzheng@besti.edu.cn, zyuan@tsinghua.edu.cn

409932748@qq.com

Abstract. SQUARE is an iterated block cipher proposed by Daemen et.al. in FSE1997. Inspired by Bogdanov et.al.'s recent works [12], we first present an improved biclique attack, i.e. stat-based independent biclique attack on full rounds SQUARE in this paper. We construct a one round stat-based independent biclique for the initial round, and utilize matching with precomputation techniques to recover the whole key from the remaining rounds. The computing complexity of our attack is $2^{126.17}$ encryptions and required data can be reduced to a single plaintext-ciphertext pair. To be the best of our knowledge, our attack has an optimal computing complexity and data complexity of biclique attack on full rounds SQUARE.

Keywords: Block cipher SQUARE, Biclique attack, Star-based independent biclique, balanced Biclique

1. Introduction

SQUARE. SQUARE is an eight rounds SPN block cipher [1] proposed by Daemen, Knudsen and Rijmen in FSE1997. As we all know, Rijndael, the candidate of Advanced Encryption Standard (AES), was also proposed by Daemen and Rijmen in 1997, SQUARE is considered as the predecessor of the AES. So all kind of cryptanalysis of AES, such as difference cryptanalysis [13], linear cryptanalysis [14], boomerang attack [2], biclique attack [3], etc, are also suitable for SQUAER. The first attack on SQUARE is a square attack [1] which is named after the block cipher SQUARE, this square attack can break six rounds SQUARE with 2^{72} encryptions, 2^{32} chosen plaintexts, and 2^{72} block of memory[1]. In 2011, Koo et.al.gave a related-key boomerang attack on full rounds SQUARE[2], they applied a three rounds related-key differentials with probability of 2^{-28} to construct a seven rounds related-key boomerang distinguisher, and successfully attacked on full rounds SQUARE with 2^{36} encryptions and 2^{123} data. In 2014, Hamid et.al first presented a single-key attack on full rounds SQUARE [3], they constructed a 3 rounds biclique using the independent related-key differentials and applied matching with precomputation on the remaining five rounds with 2^{126} encryptions and 2^{48} chosen plaintexts. This year, ZHANG et.al showed a biclique attack on full round SQUARE [15], which need about $2^{126.3}$ encryptions and 2^{16} chosen plaintexts.

Biclique attack. Biclique attack was firstly proposed by Khovratovich et.al in 2011[4]. A biclique allows an adversary to test a set of key candidates very efficiently. The biclique attack has been regarded as an advance in the fields of symmetric-key cryptography. Since its introduction, an entire rounds cryptanalysis researches emerged, aiming to apply the biclique techniques to various block ciphers [5][6][7][8][9][10]. In 2015, Bogdanov et.al. [12] proposed star biclique structures, i.e., the star-based biclique attacks, on all versions of AES cipher with the minimal possible data complexity theoretically, but their star biclique structures are not independent. Up to now, the star-based biclique attack has not been widely used.

Our contributions. Motivated by the star-based biclique attacks on AES [12], we first present a star-based independent biclique attack on full rounds block cipher SQUARE, i.e., we first give a star independent biclique structure. We construct a single round star independent biclique on the first round according to the independent related-key differentials, and apply matching with precomputation technique on the remaining seven rounds to recover the all 128 bits keys. Perhaps a star independent biclique structure could result in a best computing complexity and date complexity among other known biclique structures for full rounds block ciphers. To be the best of our knowledge, our star-based independent biclique attack on full rounds SQUARE, with $2^{126.17}$ encryptions and a single plaintext-ciphertext pair, are better than the existing results. In addition, we show that a biclique attack can be improved by changing the biclique constructions or by selecting better differences characteristics in the biclique construction.

Outline. This paper is organized as follows. In section 2, we describe the block cipher SQUARE. In section 3, we introduce star-based independent bicliques. In section 4, we present a star-based independent biclique attack on full rounds SQUARE. Finally, we give our conclusion in Section5.

2 Description of SQUARE

Here, we give a description of block cipher SQUARE.

2.1 Round Transformation

SQUARE is an eight rounds an iterated block cipher with a block length and a key length of 128 bits each. The round transformation of SQUARE is composed of four distinct transformations. Similar to AES, SQUARE is also SPN structure. The basic building blocks of the cipher are five different invertible transformations that operate on a 4×4 array of bytes. The element of a state a in row i and column j is specified as $a_{i,j}$. Both indexes start from 0. The round transformations are composed of a linear transformation θ, a nonlinear transformation γ, a byte permutation π and bitwise round key addition σ, as is depicted in Fig1.

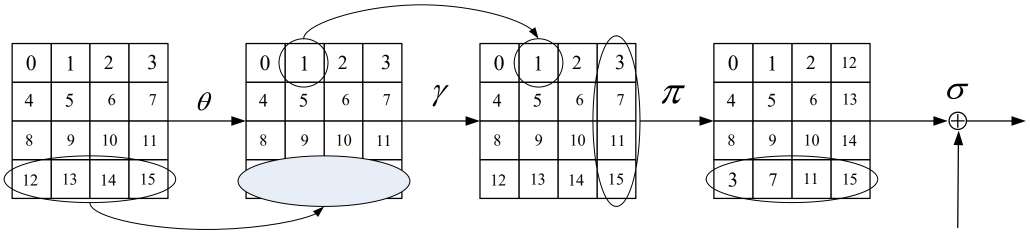

Fig1. The Round Transformation of SQUARE

A linear transformation θ. θ is a linear operation that operations separately on each of the four rows of a state. We have

$$\theta : b = \theta(a) \Leftrightarrow b_{i,j} = c_j a_{i,o} \oplus c_{j-1} a_{i,1} \oplus c_{j-2} a_{i,2} \oplus c_{j-3} a_{i,3} \qquad i, j = 0,1,2,3$$

Where the multiplication is in $GF(2^8)$ and the indices of c must be taken modulo 4. The rows of a state can be denoted by polynomials, i.e., the polynomial corresponding to row i of a state a is given by

$$a_i(x) = a_{i,0} \oplus a_{i,1} x \oplus a_{i,2} x^2 \oplus a_{i,3} x^3$$

Defined $c(x) = \oplus_j c_j x^j$, θ can be described as a modular polynomial multiplication:

$$b = \theta(a) \Leftrightarrow b_i(x) = c(x) a_i(x) \bmod 1 \oplus x^4 \qquad 0 \le i < 4$$

$c(x)$ can be denoted as a 4×4 MDS matrix M in $GF(2^8)$,where

$$M = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

A nonlinear transformation γ. γ is a nonlinear byte substitution, identical for all bytes. Every byte in the state is replaced by the byte generated after using a S-box.

$$\gamma : b = \lambda(a) \Leftrightarrow b_{i,j} = S_\gamma(a_{i,j})$$

Where S_γ is an invertible 8-bit substitution table or S-box.

A byte permutation π. π is a linear transformation transposing the state matrix. π is to interchange of rows and columns of a state.

$$\pi : b = \pi(a) \Leftrightarrow b_{i,j} = a_{j,i}$$

π is an involution, so $\pi^{-1} = \pi$.

Bitwise round key addition σ. σ is bitwise Xor. The 128-bit internal state is Xor with the 128-bit subkey:

$$\sigma[k^t] : b = \sigma[k^t](a) \Leftrightarrow b = a \oplus k^t$$

where k^t is the subkey of round t.

2.1 The Key Schedule

The key schedule of SQUARE is simple but effective. The key schedule generates 9 subkeys $rk^0, rk^1, ..., rk^8$ and each of them is 128 bits. K is the master key and rk^0 is initiated with K. $rk^{i+1}, i = 0,1,...,7$ is generated by

$$\begin{aligned} rk^{i+1}_{row(0)} &= rk^i_{row(0)} \oplus rotl(rk^i_{row(3)}) \oplus C^i \\ rk^{i+1}_{row(j)} &= rk^i_{row(j)} \oplus rk^{i+1}_{row(j-1)}, \qquad for \quad i, j = 1,2,3 \end{aligned}$$

where C^i is a round constant and the operation $rotl$ is a left-rotation operation

$$rotl[a_{i,0}, a_{i,1}, a_{i,2}, a_{i,3}] = [a_{i,1}, a_{i,2}, a_{i,3}, a_{i,0}]$$

SQUARE is defined as eight rounds preceeded by a key addition $\sigma[k^0]$ and by θ^{-1}:

$$SQUARE[k] = \rho[k^8] \circ \rho[k^7] \circ \rho[k^6] \circ \rho[k^5] \circ \rho[k^4] \circ \rho[k^3] \circ \rho[k^2] \circ \rho[k^1] \circ \sigma[k^0] \circ \theta^{-1},$$

where $\rho[k^t]$ is the round transformation

$$\rho[k^t] = \sigma[k^t] \circ \pi \circ \gamma \circ \theta$$

3 Star-based Independent Bicllique

In this section, we introduce Canteaut el.al's star-based biclique structure, and construct a star-based independent biclique from related-key differentials.

3.1 Star-based Biclique Structure

In paper[11], Canteaut el.al first proposed a biclique attack whose data complexity can be reduced to a single plaintext-ciphertext pair. They suggested that the structure of biclique with just one state in one vertex set and 2^{2d} states in the other one, rather than 2^d states in one vertex set and 2^d states in the other one. The structure of the former is called a star (See Fig2), and the latter's is called a balanced biclique (See Fig3).

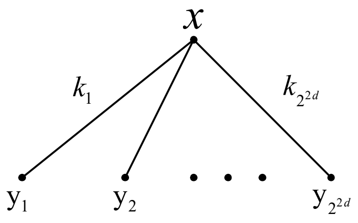

Fig2. Stars: unbalanced biclique with dimension d

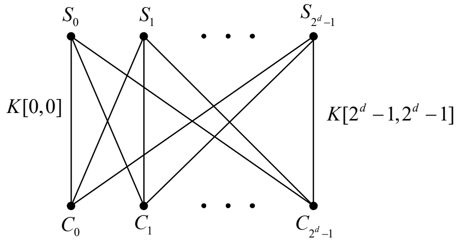

Fig3. Balanced biclique with dimension d

3.2 Constructing a Star-based Independent Biclique from Related-Key differentials

As we know, there are two approaches to construct balanced bicliques. One is from independent related-key differentials, and the other is from interleaving related-key differentials. In most cases of biclique attacks, ones always consider independent related-key differentials. Because the star-based biclique has an advantage of data complexity, we focus on constructing a star biclique from independent related-key differentials, and named this kind of biclique as a star-based independent biclique. It is worth to noting that we have implemented a star-based independent biclique attack on full rounds SQUARE in this paper. The procedure of constructing a star-based biclique is following.

Suppose we have a set of $2^d - 1$ related-key Δ - differentials from x to $y_{i,j}$:

$$(0, \Delta_i^K) \mapsto \Delta_i$$

and also have another set of $2^d - 1$ related-key ∇ - differentials from the same part of the cipher:

$$(0, \nabla_j^K) \mapsto \nabla_j$$

If the Δ - differentials and ∇ - differentials do not share any active non-linear components, i.e., both of the differentials are independent, we should construct an independent biclique.

If input x , output $y_{0,0}$ and key $K[0,0]$ also conform to both of Δ - differentials and ∇ - differentials, then the values

$$\begin{cases} x \\ y_{i,j} = y_{0,0} \oplus \Delta_i \oplus \nabla_j \\ K[i,j] = K[0,0] \oplus \Delta_i^K \oplus \nabla_i^K \end{cases}$$

form a star of dimension d , with $\Delta_0 = \nabla_0 = \Delta_0^K = \nabla_0^K = 0$. We named it as a star-based independent biclique .

4 A Star-based Independent Bicllique Attack on Full Round Block Cipher SQUARE

According to Section 3, we illustrate our star-based independent biclique attack on full rounds block cipher SQUARE in this section. We construct a single round star-based independent-biclique of SQUARE with dimension eight, and apply this star-based independent-biclique to recover all keys of full round SQUARE. Our single round star-based independent-biclique can place the initial round or final round of SQUARE. Here, we place it at the initial round.

4.1 Key Partitioning

We divide the 128-bit key K into 2^{112} groups with 2^{16} keys in each group. The index i is placed in byte 0 whereas index j is placed in byte 15. Δ - differentials activates byte 0 of key $\$0$ and ∇ - differentials activates byte 15 of key $\$0$. The base key $K[0,0]$, also the first subkey, are all 16-byte values with two bytes fixed to 0 whereas the remaining 14-bytes take all possible values (shown in Fig4). All of 2^{16} keys in a set $K[i,j]$ are defined relative to the base key $K[0,0]$, and two differentials Δ_i^K and ∇_j^K, where $i,j \in \{0,...,2^8-1\}$.

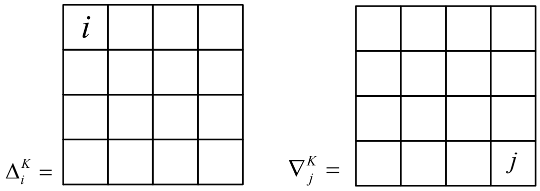

Fig4. key partitioning

4.2 Constructing a Single Round Star-based Independent-Biclique

Step1-base computation. Let x_0 be the plaintext, obtain $y_{0,0} = f_{K[0,0]}(x_0)$ under the base key $K[0,0]$, where f is the subcipher that cover the star-based independent-biclique (Fig5. left).

Step2-Δ-differentials computation. Under 2^8-1 key differences Δ_i^K ($i \in \{0,...,2^8-1\}$), get $0 \xrightarrow{\Delta_i^K} \Delta_i$ (Fig4. middle). This process has the same starting point as the base computation.

Step3-∇-differentials computation. Under 2^8-1 key differences ∇_j^K ($j \in \{0,...,2^8-1\}$), get $0 \xrightarrow{\nabla_j^K} \nabla_j$ (Fig4. right) from the same part of the SQUARE cipher, i.e., this process has the same starting point as the base computation.

Step4- biclique computation. Both the differentials do not share any non-linear components, we can combine both the differentials into a combined differentials. Then the values

$$\begin{cases} x & \\ y_{i,j} = y_{0,0} \oplus \Delta_i \oplus \nabla_j & \Delta_0 = \nabla_0 = 0 \\ K[i,j] = K[0,0] \oplus \Delta_i^K \oplus \nabla_i^K & \Delta_0^K = \nabla_0^K = 0 \end{cases}$$

form an star with dimension eight. As is depicted in Fig5, the differences propagation in these two differences over one round is non-overlapping, so we could obtain a star-based independent biclique.

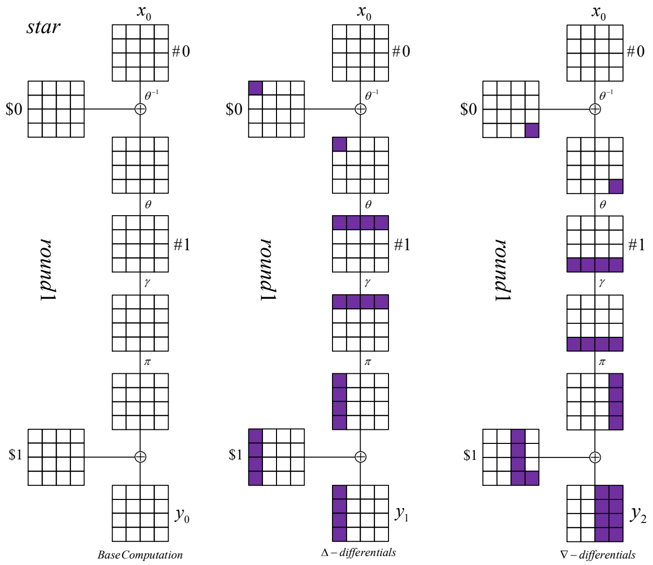

Fig5. Star over first round

4.3 Matching with Precomputation

Here, we choose to match on byte 0 in the state after byte permutation transformation π of round 4. For the forward direction of matching, in round 2, no S-boxes is to be recomputed. In 3-th round, four S-boxes have to be recomputed. In 4-th round, one S-boxes need to be recomputed. So there are 5 S-boxes to be recomputed in the forward matching (Fig6. top). For the backward direction of matching, in 5,6,7,8-th round, four S-boxes, sixteen S-boxes, eight S-boxes, three S-boxes need to be recomputed, respectively. Hence, there are in total 36 S-boxes to be recomputed.

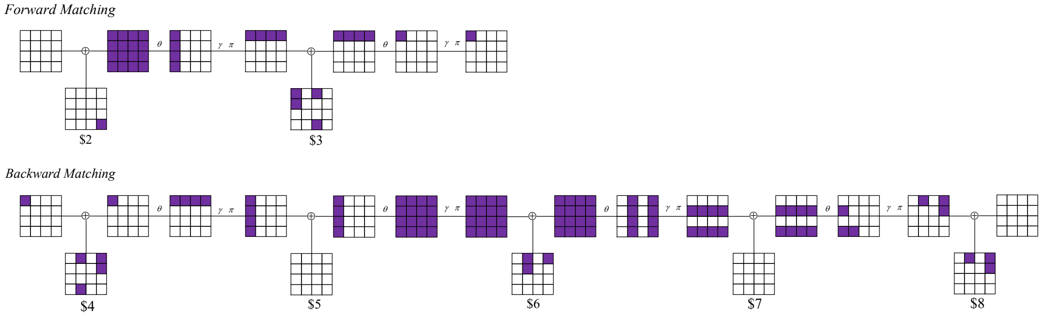

Fig6. Matching with Precomputations

4.4 Complexities of the Attack

Computing complexity. The full round SQUARE cipher has 16*8=128 S-boxes. From section 4.3, the matching with precomputation process yields a recomputation of 36 out of 128 S-boxes.

Thus, the recomputation needs $C_{recomp} = 2^{16} \cdot \frac{36}{128} \approx 2^{14.17}$ encryptions, while the precomputation needs $C_{precomp} = 2^{8} \cdot \frac{7}{8} \approx 2^{7.81}$ encryptions. The constructing one star-based independent-Biclique needs $C_{biclique} = 2 \cdot 2^{8} \cdot \frac{1}{8} \approx 2^{6}$ encryptions. The eliminating false positives needs $C_{falsepos} = 2^{8}$ encryptions. Therefore, the computing complexity of our star-based independent biclique attack on full rounds SQUARE is

$$\begin{aligned} C_{full} &= 2^{n-2d} \cdot (C_{recomp} + C_{biclique} + C_{precomp} + C_{falsepos}) \\ &\approx 2^{112} \cdot (2^{14.17} + 2^{6} + 2^{7.81} + 2^{8}) \\ &\approx 2^{126.17} \end{aligned}$$

Data complexity. For our star-based independent biclique attack on full rounds SQUARE, the minimal data complexity is theoretically attainable, which can be reduced to a single known plaintext-cihpertext pair. One known plaintext-ciphertext pair can sometimes be enough. Two known plaintext-ciphertext pairs yield a success probability of practically 1.

Memory complexity. The memory complexity is upper bounded by 2^{8} computing of subcipher involved in the precomputation stage.

5 Conclusions

In this paper, we introduce a star-based independent bicliques attack, and first propose a star-based independent biclique attack (balanced biclique) on full rounds block cipher SQUARE. Our attack could reduce the data complexity to the theoretically attainable minimum. In our attack, we construct a single round star-based biclique on the first round of SQUARE and apply matching with precomputation on the remaining seven rounds. The computing complexity of our attack is about $2^{126.17}$ encryptions, and the data complexity can be reduced to a single plaintext-ciphertext pair. Compared with the existing biclique attacks on full rounds SQUARE, both the computing complexity and data complexity of our attack are optimal. Additionally, we can note that the structure of biclique perhaps play an important role in reducing the data complexity.

Reference

[1] Daeman, J., Knudsen, L.R., Rijmen, V.: The Block Cipher SQUARE. In: Biham, E. (ed.) FSE'97. LNCS, vol. 1267, pp. 149-165. Springer, Heidelb erg, 1997.

[2] Koo, B., Yeom, Y., Song, J.: Related-Key Boomerang Attack on Block Cipher SQUARE. IEICE Transaction, 94-A(1), 3-9, 2011.

[3] Hamid Mala,V.: Biclique Cryptanalysis of the Block Cipher SQUARE. Let Information Security, 2014.8(3): 207-212.

[4] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique Cryptanalysis of the Full AES. Cryptology ePrint Archive, Report 2011/449, 2011. http://eprint.iacr.org/

[5] Farzaneh Abed, Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel. Biclique Cryptanalysis Of PRESENT, LED and KLEIN. Cryptology ePrint Archive, Report 2012/591, 2012. http://eprint.iacr.org/2012/591.

[6] Shao-zhen Chen and Tian-min Xu. Biclique Attack of the Full ARIA-256. Cryptology ePrint Archive, Report 2012/011,2012. http://eprint.iacr.org/2012/011.

[7] Mustafa C¸ oban, Ferhat Karako¸c, and Ozkan Boztas. Biclique cryptanalysis of TWINE. In Josef Pieprzyk, Ahmad-Reza¨ Sadeghi, and Mark Manulis, editors, Cryptology and Network Security, 11th International Conference, CANS 2012, Darmstadt, Germany, December 12-14, 2012. Proceedings, volume 7712, pages 43-55. Springer, 2012.

[8] Deukjo Hong, Bonwook Koo, and Daesung Kwon. Biclique attack on the full HIGHT. In Howon Kim, editor, Information Security and Cryptology-ICISC 2011-14th International Conference, Seoul, Korea, November 30-December 2, 2011. Revised Selected Papers, volume 7259 of Lecture Notes in Computer Science, pages 365-374. Springer, 2011.

[9] Takanori Isobe and Kyoji Shibutani. Security Analysis of the Lightweight Block Ciphers XTEA, LED and Piccolo. In Willy Susilo, Yi Mu, and Jennifer Seberry, editors, Information Security and Privacy-17th Australasian Conference, ACISP 2012, Wollongong, NSW, Australia, July 9-11, 2012. Proceedings, volume 7372 of Lecture Notes in Computer Science, pages 71-86. Springer, 2012.

[10] Yanfeng Wang, Wenling Wu, and Xiaoli Yu. Biclique cryptanalysis of reduced-round piccolo block cipher. In Mark Dermot Ryan, Ben Smyth, and Guilin Wang, editors, Information Security Practice and Experience-8th International Conference, ISPEC 2012, Hangzhou, China, April 9-12, 2012. Proceedings, volume 7232 of Lecture Notes in Computer Science, pages 337–352. Springer, 2012.

[11] Canteaut, A ., Naya -Plasencia, M., Vayssi`ere, B.: Sieve-in-the-middle: improved MITM attacks (full version). Cryptology ePrint Archive, report 2013/324 (2013) http://eprint.iacr.org/2013/324

[12] Andrey Bogdanov,Donghoon Chang, Mohona Ghosh et al. Biclqiues with minimal Data and Time Complexity for AES.ICISC2014.

[13] Biham,E., Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard. Springer, Heidelb erg,1993.

[14] Matsui, M.: Linear cryptanalysis method for DES cipher. In: EUROCRYPT'93, LNCS, vol. 765, pp. 386-397.Springer, 1993.

[15] ZHANG Shugang,CHEN Shaozhen.Biclique Cryptanalysis of Full Round Square with Low Data Complexity. Journal of Information Engineering University. 1671-0673.2015.04.002.

Appendix A

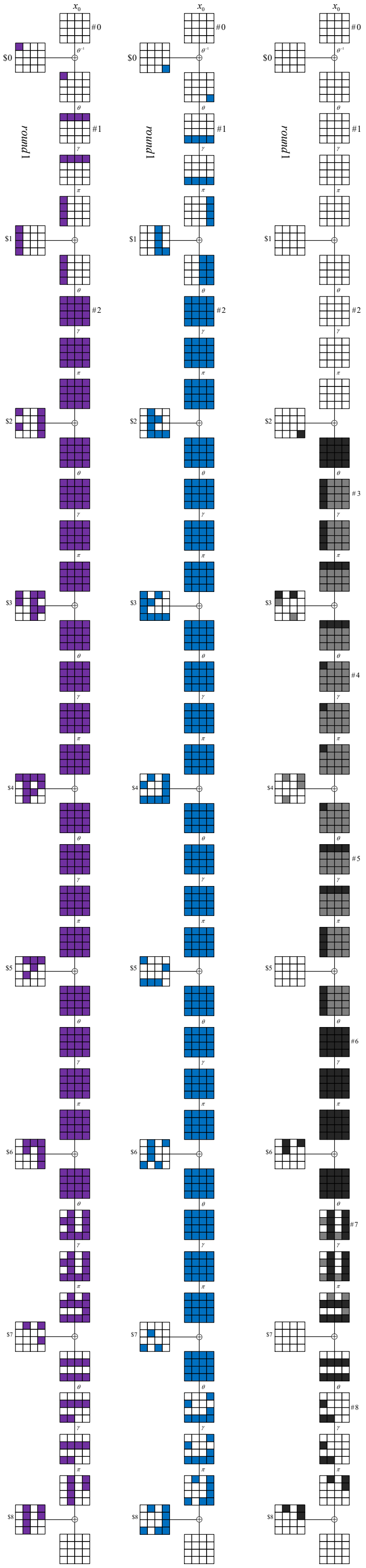

Fig7. Biclique differentials and matching in full round SQUARE